Remarks

In response to the Office Action dated April 20, 2007, Applicant respectfully requests reconsideration based on the above claim amendment and the following remarks. Applicant respectfully submits that the claims as presented are in condition for allowance. Claims 1, 14, 25, 36, 43, 49, 60, 69, 78, and 84 have been amended. The claims have been amended to clarify that the packet state includes a congested state and that the congested state is a value detected in, read from and/or specified by the contents of a packet. Support for these amendments may be found on page 11 in the Specification. No new matter has been added.

Claim Rejections - 35 U.S.C. §103

Claims 1-5, 7-39, and 41-52 and 54-87 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Sharon (U.S. Pat. 6,137,782), in view of Wan (U.S. Pat. 6, 529,475) and further in view of Messinger et al. (U.S. Pat. 6,687,750). The rejection of these claims is respectfully traversed.

Amended independent claim 1 specifies a method of monitoring a packet-switched network using traffic logs. The method includes: (a) creating a histogram file; (b) generating a traffic log at a first location within the network based upon detection of the contents of a packet, the traffic log containing a plurality of values detected within the packet, the plurality of values being read from the packet including a network entry point of the packet, a network exit point of the packet, and a packet state, wherein the packet state includes a congested state which is specified by the contents of the packet; (c) transferring the traffic log from the first location to a second location; (d) storing the traffic log generated by the packet-switched network at the second location; (e) analyzing the stored traffic log to determine the time of creation of the traffic log and the network packet-switched entry and exit points of the packet; and (f) updating the histogram file using at least the time of creation of the traffic log, at least the packet state and at least one of the entry and exit points of the packet, wherein the histogram file is utilized to monitor network conditions in near real-time enabling the detection and correction of network overloads and congestion at one of a network node and network node link before network customers are affected.

It is respectfully submitted that the combination of Sharon, Wan and Messinger fails to describe each and every of the features specified in amended independent claim 1. For example, the cited references fail to describe generating a traffic log at a first location within the network based upon detection of the contents of a packet, the traffic log containing a plurality of values detected within the packet, the plurality of values being read from the packet including a network entry point of the packet, a network exit point of the packet, and a packet state, wherein the packet state includes a congested state which is specified by the contents of the packet

In the Office Action, the Examiner has conceded that Sharon does not describe that the packet state includes a congested state. (See Page 3). The Examiner then asserts that Wan describes extracting information from the network packet thereby determining the congestion of the network. The Office Action continues on to assert that it would then be obvious to one of ordinary skill in the art to "determine the congestion state of the packet for the purpose of improving [the]flow of data". Applicants respectfully but completely disagree with the implied assertion that Wan describes a packet state that includes a "congested" state or that Wan describes the concept of a "congested state" value at all.

The salient error in this assertion, among others, appears to be that the operation/purpose of a Real Time Control Packet ("RTCP) described in Wan has apparently been equated by the Office Action to the data packet recited in the claims. It should be noted that the RTCP protocol discussed in Wan is a modification of the User Datagram Protocol/IP ("UDP") because, unlike the ubiquitous TCP/IP protocol, UDP does not have any inherent congestion control mechanism.

Applicant, respectfully points out that *Wan simply* does not describe that a RTCP packet has a "congested state" value that can be detected in or read from a RTCP packet. Wan describes that RTCP information is used to build a congestion control mechanism (Col. 5, l. 62-63) that is based on the periodic transmission of only RTCP control packets (Col. 6, l. 5-8). According to Wan, the congestion monitors merely perform basic processing of control packets to collect statistical information. (Col. 6, l. 54-56). RTCP packets provide sufficient information **to derive** statistics such as the packet loss rate, average payload size, connection through put, and determine if problems are local or global. (Col. 8, l. 11-16). Such information is then used by a central server to ultimately determine the congestion of the network. (Col. 8, l. 48-51). Although bits of information from a multitude of RTCP packets may be statistically analyzed to ultimately determine network congestion by a congestion control mechanism, RTCP packets are not described in Wan as containing any such value that is a packet state that includes a "congested" state. As such, Applicant respectfully asserts that Wan fails to describe the subject matter asserted by the Office Action to Wan and that Wan, therefore, fails to cure the conceded deficiency of *Sharon*.

Messinger discusses a network traffic visualization application which enables the rapid assimilation of substantial amounts of information involving the activities of various network components. The extracted data is then compiled into an information file and stored for display at stated times or at the request of a network administrator. Messinger does not describe a packet state that includes a "congested" state value that can be detected in or read from a packet. As such, *Messinger* also fails to cure the conceded deficiency of *Sharon*.

For at least the above reasons Wan and Messinger fail to disclose the conceded deficiencies of *Sharon*. As such, the Examiner has failed to meet her burden to establish a prima facie case for obviousness for at least this reason since the combination of references fails to describe each and every claim element. As such, claim 1 and its dependents are allowable over the combination of Sharon, Wan and Messinger. Independent claims 14, 25, 49, 60, 69, 78 and their dependents contain similar recitations and are also allowable for at least the same reasons.

Further, Claim 1 recites, in pertinent part, "generating a traffic log at a first location within the network based upon detection of the contents of a packet, the traffic log containing a plurality of values detected within the packet, the plurality of values being read from the packet including a network entry point of the packet [and] a network exit point of the packet…" The Office Action asserts the *Sharon* describes "analyzing the network entry and exit points of the packet" and specifically cites Column 8, lines 10-30 in support.

Applicant respectfully points out that the cited portion of *Sharon* actually describes that the "network parser 34 analyzes the header in each received packet for source and destination [IP] address…" Applicants respectfully assert that analyzing source and destination addresses does not describe a plurality of values being detected within a packet, the plurality of values being read from the packet including a network entry point of the packet [and] a network exit point of the packet.

A source and a destination IP/MAC address is not necessarily a network entry or exit point. In being transmitted from the source address to a destination address, the packet may transit within or across one or more networks. The packet source and destination address has no particular correspondence with the packet's entry or exit point of the network. The source and destination addresses are different and broader concepts from an entry and exit point of a network. For at least this reason, Sharon fail to describe the subject matter asserted to Sharon by the Office Action.

Wan, discussed above, deals only with RTCP packets. Wan does not describe a value being detected that is a network entry or exit point of a packet. As such, Wan does not cure this deficiency of Sharon.

Messinger, discussed above, concerns a network traffic visualization application which enables the rapid assimilation of information by extracting traffic data between a starting time and an ending time. However, Messinger fails to describe values being detected that are a network entry and exit point of a packet. As such, Messinger also fails to cure the deficiencies of Sharon.

For at least the above reason the combination of Sharon, Wan and Messinger fails to describe that "…upon detection of the contents of a packet, the traffic log containing a plurality of values detected within the packet, the plurality of values being read from the packet including a network entry point of the packet [and] a network exit point of the packet…" As such, the Office Action has failed to establish a prima facie case for obviousness for at least this reason since the combination of references fails to describe each and every claim element. As such, claim 1 and its dependents are allowable over the combination of Sharon, Wan and Messinger. Independent claims 14, 25, 43, 49, 60, 69, 84 and their dependents contain similar subject matter and are also allowable for at least the same reason.

Furthermore, Claim 1 recites, in pertinent parts, creating a histogram file, analyzing the stored traffic log to determine the time of creation of the traffic log…and updating the histogram file using at least the time of creation of the traffic log… wherein the histogram file is utilized to monitor network conditions in near real-time…" The Office Action concedes on page 3 that the sub-combination of Sharon and Wan fails to describe these recitations. The Applicant respectfully asserts that Messinger also fails to describe the above recitations.

Messinger discusses that extracted data is compiled into a network information file after a specified network monitoring interval and then is subsequently displayed (Col. 3, l. 30-50). *Messenger* further teaches that the user uses a GUI to create filtering expressions for **extracting the desired information** from the network information files. Thus, Messinger does not discuss using a histogram file to monitor network conditions in **near real-time** as the user must manually filter the network information file to obtain the desired data. Thus, in Messinger, the administrator must wait until after the monitoring has been concluded, must wait until after the collected information has been compiled into a file, and then must wait until the compiled file has been filtered manually by a user before the desired data may be displayed to the user at one of a stated time or upon request. Thus, Messinger does not disclose using a histogram file to monitor network conditions in **near real-time**. Manual information extraction would necessarily preclude presenting the information in near real-time due to the inherent delay involved in manual process.

Therefore, Messinger fails to describe the subject matter asserted to Messinger by the Office Action to cure the conceded deficiencies of the sub-combination of Sharon and Wan. As such, Applicant respectfully asserts that the Examiner has failed to meet her burden to establish a prima facie case for obviousness for at least this reason since Messinger fails to cure the conceded deficiencies of Sharon and Wan. As such, combination of Sharon, Wan and Messinger fails to describe each and every claim element and claim 1 and its dependents are allowable over the combination of Sharon, Wan and Messinger for at least this reason. Independent claims 14, 25, 43, 49, 60, 69, 78, 84 and their dependents recite similar subject matter and are allowable for at least the same reasons.

In regards to amended independent claim 36, amended independent claim 36 recites in pertinent part, that the packet includes one of the following data elements: an "OK" state, an "illegal" state, a "congested" state and an "error" state. Applicants respectfully assert that none of Sharon, Wan, Messinger or their combination describes that the packet includes one of the following data elements: an "OK" state, an "illegal" state, a "congested" state and an "error" state. As such, a prima case of obviousness has not been established and amended independent claim 36 is allowable for at least this additional reason.

Conclusion

In view of the foregoing amendments and remarks, this application is now in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is invited to call the Applicants' attorney at the number listed below.

The present Amendment is being filed with an RCE. No additional fees are believed due. However, please charge any additional fees or credit any overpayment to Deposit Account No. 50-3025.

Respectfully submitted,

Date: July 20, 2007

/Arno T. Naeckel/
Arno T. Naeckel

Withers & Keys, LLC
P.O. Box 71355
Marietta, GA 30007-1355
(770) 518-9822